Comparison of Forwarding Strategies in Internet Connected MANETs

Erik Nordström[a] *erik.nordstrom@it.uu.se*
Per Gunningberg[a] *per.gunningberg@it.uu.se*
Christian Tschudin[b] *christian.tschudin@unibas.ch*
[a]Department of Information Technology, Uppsala University, Sweden.
[b]Computer Science Department, University of Basel, Switzerland.

For efficient Internet Connectivity in MANETs, multiple gateways and potentially multi-homing and hand-over need to be supported. We compare two forwarding strategies; default routes and tunneling to gateways. We find that tunneling is more efficient and flexible compared to default routes. In fact, we show that default routes will not operate correctly in some situations, particularly in multi-homed networks with more than one gateway.

I. Introduction

For many years now, researchers have been working on routing protocols for mobile ad hoc networks (MANETs). However, the focus has mainly been to improve efficiency of routing algorithms for operation in disconnected ad hoc networks, while interoperability with other networks (e.g., the Internet) has seen less attention.

MANETs are often envisaged to have flat addressing (no prefixes) and flat routing. When mobile nodes connect to the Internet, there may be multiple gateways that offers that service. This dynamic environment is challenging for ad hoc nodes that want to make use of the services that the gateways offer. For example, consider a scenario where several gateways are accessible to a visiting ad hoc node and Mobile IP(v4) is used to redirect its return traffic from the home network. In this scenario, the ad hoc node needs to track which gateway its packets in the forward flow are currently being forwarded to. Since there may be multiple hops to the gateways, an unsolicited gateway change at an intermediate node may break the source node's return traffic flow, because it will not be triggered to re-register with the Mobile IP foreign agent at the new gateway.

Another problem is related to addressing. Consider an ad hoc network where the IP addresses of nodes are strictly used as identifiers without any prefix semantics. This might be the case if visiting nodes use their home addresses in a foreign ad hoc network where one or more Mobile IP foreign agent gateways hide these "alien" prefixes behind one or more care-of-addresses. With such a mix of addresses and the combination of reactive routing there is a resolution problem. A node can not assume that a packet should be forwarded to a gateway just because there is a default route and no other matching host route in its routing table. It must first flood the network with a route resolution request to eliminate the possibility that there is a node in the ad hoc network with the destination address of the target. Furthermore, if the path to the gateway is multiple hops, this resolution problem will re-occur at each intermediate node, unless the source node can somehow delegate its information about the destination to other nodes in the network.

In this paper we review some of the proposals for Internet connectivity with regard to the forwarding strategy used and how they handle or do not handle the scenarios described above. We identify mainly three classes of forwarding strategies among these proposals; *host routes*, i.e., one explicit routing entry for each destination, *default routes* that aim to provide route aggregation and *tunneling* that encapsulates packets for the Internet with a gateway's address. However, we focus on the two latter strategies, because they are more widely proposed and aim to provide the most benefits.

Our contribution is the comparison of default routes and tunneling and the identification of problems to solve for their efficient operation. We apply the two strategies to reactive routing (e.g., AODV [6]) where we compare the transparency to routing protocols, ability to handle multiple gateways (for multi-homing and hand-over), the overhead and performance using ns-2 simulations. We conclude that tunneling (or other methods using a routing header, e.g., source routing), is more efficient and handles multiple gateway scenarios without extra signaling or protocol logic.

This paper is structured as follows. In section II we discuss related work. Section III and IV discuss the default route and tunneling approaches in more detail. In section V we evaluate the two strategies in simulation, while we conclude the paper in section VI.

II. Related Work

In this section we review the main proposals for MANET Internet connectivity.

Globalv6 by Wakikawa et al. [9], can work with Mobile IP, but it is not mandatory. Globally routable IP addresses can be acquired by IPv6's auto-configuration mechanism. Routing towards the gateway is done on a hop-by-hop basis using a default route. In section I we described how such a solution could suffer from repeated route discovery floods. This is also pointed out by Nilsson et al. in [5] and could be very inefficient. However, in Globalv6, these cascading effects are avoided by requiring intermediate nodes to configure host route entries in the route setup phase. The consequence of this requirement is that route aggregation is lost. Maintaining host route entries in this way also suffers from a state replication problem. Missing host route states at nodes severely impacts the performance and the correct operation of this default route solution, as we show in section V. In addition, this solution also suffers from the inability to track gateway changes – the default route could change to point to a new gateway at an intermediate node – leaving an upstream node further away from the gateway unaware of this update. Hence it will not be triggered to re-register at the new foreign agent and its return packet flow might be lost at the old gateway. Although we have identified these inefficiencies (further discussed in the next section), we would like to point out that there may be ways to solve these problems, but that it likely requires additional protocol logic and possibly signaling between gateways.

Jönsson et al. studies in [4] the integration of Mobile IP in MANETs. They describe a system called MIPMANET where tunneling from ad hoc nodes to the foreign agent is used to achieve default route like behavior. However, in contrast to the work presented in this paper, the main result is the effect of using unicast or broadcast transmissions for periodic agent advertisements. A similar solution to MIPMANET is suggested by Ratanchandani et al. in [7].

Gateway discovery in NAT'ed on-demand MANETs is studied in [2], where Engelstad et al. find that tunneling to gateways avoids race conditions from proxy route replies in the presence of multiple gateways. This is in line with our findings as well. In fact, they used our AODV-UU [1] tunneling implementation for their study.

The Dynamic Source Routing protocol (DSR) [3] is interesting because it supports the type of indirection that tunnels provide to operate efficiently with (multiple) gateways. Tunnels would transparently work also with DSR, but it would be an unnecessary addition.

We also point to the LUNAR protocol [8] which tunnels *all* network traffic directly over the wireless link layer. Because LUNAR creates a complete one-hop illusion to the IP layer, gateway connectivity is easy to support.

In the following sections we will more closely examine the relative merits or drawbacks of the default route or tunneling approaches proposed in related work.

III. Default Routes

The idea of a default route as a generic routing table entry is common in LANs, where there is one gateway one hop away with subnet addressing. However,

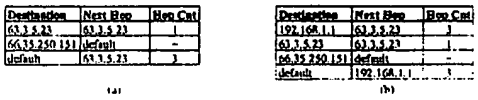

Figure 1: Two different routing table configurations to the same end. The address 66.35.250.151 is a destination on the Internet.

MANETs often have flat addressing and multiple gateways several hops away. To adapt the default route concept to the MANET environment, host route table entries need to be added to avoid repeated route look-ups on source as well as intermediate nodes (figure 1 (a)). Furthermore, multiple gateways are not easily supported, since there is only one default route and no way to track gateways in the routing table. Hence, there is no possibility to support multi-homing or efficient hand-over. In Globalv6 [9], the routing table configuration shown in figure 1 (b) is proposed. The default route is now mapped to a gateway and host routes point to the default route. We note that this increases the required routing table accesses to three for each packet forwarded to a gateway and may be inefficient. Precomputing the host to next hop mapping does not always help, because most reactive protocols require each entry to be accessed and refreshed when a packet is forwarded.

We have already touched upon the default route solution's problems with tracking gateway changes and to keep consistent states in the network. We will now describe these problems in more detail.

III.A. Gateway Tracking Problem

As already pointed out in previous sections, a default route can be re-pointed to another gateway on down-

stream nodes (figure 2). This will break connections when using a gateway running NAT or Mobile IP, because the return packet flow will be sent to the old gateway.

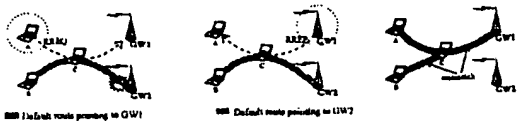

Figure 2: Problem tracking the gateway. A source node (B) may not be notified of a default gateway change triggered by a reactive routing protocol's route request (RREQ) and route reply (RREP) exchange.

However, with the routing table in figure 1 (b), a node can tell when a default route is re-pointed to a new gateway, since there is a default route → gateway mapping. But extra routing logic needs to be added to handle this. For example, to drop route replies conflicting with an existing default route.

Another option is to handle the redirection of the return packet flow by signaling between the gateways. An unsolicited gateway change in the default route might then prove efficient, because each source node using the default route does not have to be notified and possibly will not have to rediscover a route to the new gateway.

III.B. State Replication Problem

To avoid cascading route requests, intermediate nodes must gather all the host → default route mappings of upstream nodes when the default route is repaired or updated. In figure 3, node A is communicating with Internet hosts through gateway (GW). A's host route state S_A is not replicated when node B repairs the route to GW. Node D will not be able to forward packets to host(s) represented by state S_A.

Figure 3: Example of state replication problem with default routes.

Extra protocol logic needs to be added to properly handle the replication of the necessary state in the routing tables of intermediate nodes. In section V, we show by simulation that non-replicated state has serious negative impact on the efficiency of a default route solution.

IV. Tunneling

With tunneling, an encapsulated packet from an ad hoc node for an Internet destination is sent to the gateway using the gateway's explicit IP address and the IP forwarding mechanism as configured by the ad hoc routing protocol. At the gateway, the packet will exit the tunnel and is decapsulated. Return traffic inbound at the gateway does not need to be tunneled, since the return IP address (the ad hoc source node's home address) is routable within the ad hoc network.

The main advantage of a tunneling solution is that the source node of a flow is always in full control and alone carries all the state necessary to forward a packet to a gateway. No state is replicated at intermediate nodes, except the state for the route to the gateway. This makes tunneling transparent to existing routing protocols and route aggregation is achieved at intermediate nodes. In case a gateway route breaks, the source node will be notified by the routing protocol, or in case the route is repaired, an alternative route to the same gateway will be found, because the route is explicit (in contrast to a "generic" default route). This makes it easy to integrate with Mobile IP, since re-registrations are not a problem.

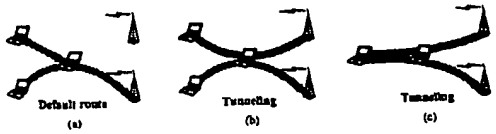

Figure 4: (a) A default route points to only one gateway at once. (b) With tunneling two nodes can share an intermediate hop while still maintaining tunnels to different gateways, (c) or one node can have tunnels to two gateways at once.

Another important property of tunneling is that it efficiently can make use of multiple gateways for the benefit of multi-homing (to achieve fault tolerance of load balancing) or performing soft hand-overs (see figure 4). In terms of routing table look-ups, tunneling is also more efficient than the default route counterpart. A source node needs to perform two look-ups in the routing table. On intermediate nodes, only one regular look-up is needed.

A disadvantage of tunneling is the overhead of encapsulation, which could be large for small data packets. However, in our implementation we use minimal IP encapsulation, resulting in the small overhead of 8 bytes per packet on egress flows only.

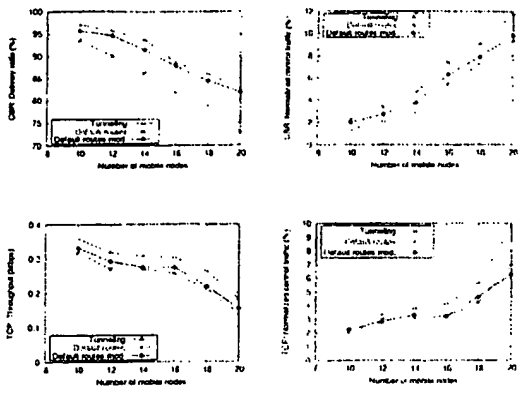

Figure 5: CBR delivery ratio and TCP throughput with normalized control traffic.

V. Evaluation

We evaluate default routes and tunneling in simulation. The simulated network has fixed density (i.e., the size grows with the number of nodes), two gateways and 10 to 20 mobile nodes. Gateways are MIP agents and two ad hoc nodes communicate with an Internet host. Results are averaged over 50 randomly generated scenarios with random waypoint mobility. We have integrated both Globalv6-style default routes and tunneling with the AODV-UU [1] implementation. Since we only have traffic for the gateways, we provide results with a default route version that always forwards all packets on the default route. This provides a reference for how default routes would work without state replication problems. A *proxy route reply* solution is used for gateway discovery.

The results for CBR traffic show that tunneling achieves the best performance (figure 5), while default routes have problems. The improved results for the modified default routes indicate that the bad performance is caused mainly by the state replication problem, since there is no return traffic that could be affected by the lack of gateway tracking.

Looking at TCP performance, the modified default route forwarding is not as much of an improvement over regular default routes. Gateway tracking is more important for TCP (i.e., two-way traffic). The reduced routing overhead of default routes supports this view – when the TCP acknowledgments are lost, TCP goes into a timeout which reduces the overall traffic. With default routes, nodes may think that they are forwarding packets to a specific gateway, when in fact they are not. Therefore, they will never re-register with the agent at the new gateway. Further simulations have verified this hypotheses. Tunneling does not suffer from the gateway tracking problem and therefore delivers more packets, which in turn increases the amount of *normalized* control traffic.

VI. Conclusion

A robust forwarding strategy is necessary to build Internet connectivity solutions for MANETs. We have compared the efficiency of using default routes to that of using tunneling. Our conclusion is that tunneling packets to a gateway in ad hoc networks with flat addressing and reactive routing is more efficient and flexible compared to default routes. In fact, we found default route forwarding – as suggested in several proposals – to not operate correctly in some situations, particularly with multiple gateways. This has adverse effects on two-way traffic, for example TCP. A tunneling solution has the potential to efficiently exploit multiple gateways for the benefit of multi-homing or for performing soft hand-overs.

References

[1] The AODV-UU implementation webpage. `http://www.docs.uu.se/scanet/aodv`.

[2] P. Engelstad and G. Egeland. NAT-based Internet connectivity for on-demand ad hoc networks. In *WONS2004*, pages 344–358, 2004.

[3] D. B. Johnson, D. A. Maltz, and Y. Hu. The dynamic source routing protocol for mobile ad hoc networks (DSR), April 2003. IETF Internet Draft, draft-ietf-manet-dsr-09.txt, (work in progress).

[4] U. Jönsson, F. Alriksson, T. Larsson, P. Johansson, and G. Q. Maguire Jr. MIPMANET - Mobile IP for Mobile Ad hoc Networks. In *1st ACM international symposium on Mobile ad hoc networking and computing (Mobihoc'00)*, 2000.

[5] A. Nilsson, C. E. Perkins, A. J. Tuominen, R. Wakikawa, and J. T. Malinen. AODV and IPv6 Internet access for ad hoc networks. *Mobile Computer and Communications Review*, 6(3):102–103.

[6] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on-demand distance vector (AODV) routing, July 2003. IETF Internet RFC 3561.

[7] P. Ratanchandani and R. Kravets. A hybrid approach to internet connectivity for mobile ad hoc networks. In *IEEE WCNC*, 2003.

[8] C. Tschudin. Lightweight Underlay Network Ad hoc Routing (LUNAR) Protocol. IETF Internet draft, draft-tschudin-manet-lunar-00.txt, March 2004.

[9] R. Wakikawa, J. Malinen, C. Perkins, A. Nilsson, and A. Tuominen. Global connectivity for IPv6 mobile ad hoc networks, (work in progress), October 2003. IETF Internet Draft, draft-wakikawa-manet-globalv6-03.txt.